

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Грובה Татьяна Ивановна

Должность: и.о. декана факультета математики и компьютерных наук имени профессора Н.И. Червякова

Дата подписания: 19.06.2026 15:22:53

Уникальный программный ключ:

bd39d4208aa94cf4422feb787c81619d42de79a7

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего
образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета математики
и компьютерных наук
имени профессора Н.И. Червякова
Грובה Т.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Криптоанализ с помощью программных средств

Направление подготовки
Направленность (профиль)

10.04.01 Информационная безопасность
Математическое и программное обеспечение
защиты информации

Год начала обучения

2026

Форма обучения

очная

Реализуется в семестре

3

Разработано

Калмыков И.А., доцент кафедры
вычислительной математики и кибернетики

Ставрополь 2026 г.

1. Цель и задачи освоения дисциплины (модуля)

Государственный общеобразовательный стандарт высшего профессионального образования Российской Федерации, формирующий государственные требования к минимуму содержания и уровня подготовки специалистов, включает обязательную дисциплину под названием «Криптоанализ с помощью программных средств».

Цель дисциплины «Криптоанализ с помощью программных средств» состоит в формировании набора общепрофессиональных компетенций магистра по специализации, а также формирование знаний, умений и навыков работы с современными технологиями обеспечения безопасности.

Дисциплина «Технологии обеспечения информационной безопасности» направлена на повышение уровня практического владения методами обеспечения информационной безопасности у обучающихся по специальности 10.04.01. Информационная безопасность. Освоение дисциплины должно способствовать решению следующих задач, встречающихся в профессиональной деятельности:

- формирование фундаментального понимания обучающимися математических основ криптографии и криптоанализа;
- формирование навыков анализа криптографических систем на предмет наличия уязвимостей;
- формирование навыков программной реализации вычислительных алгоритмов, используемых в криптографии и криптоанализе.

2. Место дисциплины (модуля) в структуре образовательной программы

Данная дисциплина относится к обязательным дисциплинам вариативной части Б1.В.07 программы магистратуры. Ее освоение происходит в 3 семестре.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ПК-3. Способен проводить инструментальный анализ защищенности компьютерной системы и осуществлять поиск уязвимостей программного обеспечения	ИД-1 ПК-3 выполняет анализ защищенности компьютерных систем с использованием сканеров безопасности	Анализирует защищённость компьютерной системы с помощью сканера безопасности
	ИД-2 ПК-3 выполняет анализ защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей	Осуществляет анализ защищенности сетевых сервисов с использованием средств автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей
ПК-5. Способен выполнять автоматизированную информационно-аналитическую поддержку	ИД-1 ПК-5 формализует задачи автоматизированной информационно-аналитической поддержки процессов принятия решений в сфере безопасности в конкретной предметной области	Применяет систему поддержки принятия решения в требуемой предметной области

процессов принятия решений в профессиональной деятельности	ИД-2 ПК-5 решает задачи прогнозирования, планирования, выработки решений при различной априорной неопределенности имеющейся информации	Осуществляет решение задачи прогнозирования и планирования в условиях неопределенности
	ИД-3 ПК-5 оценивает эффективность и качество в задачах прогнозирования, планирования, принятия решений при различной априорной неопределенности имеющейся информации	При принятии решения способен оценить эффективность и качество

4. Объем учебной дисциплины (модуля) и формы контроля *

Объем занятий: всего: 4 з.е. 108 астр.ч.	ОФО, в астр. часах
Контактная работа:	54
Лекции/из них практическая подготовка	27
Лабораторных работ/из них практическая подготовка	
Практических занятий/из них практическая подготовка	27
Самостоятельная работа	54
Формы контроля	
Экзамен	
Зачет	+
Зачет с оценкой	
Расчетно-графические работы	
Курсовая работа	
Контрольные работы	

* Дисциплина (модуль) предусматривает применение электронного обучения, дистанционных образовательных технологий (если иное не установлено образовательным стандартом)

5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием количества часов и видов занятий

№	Раздел (тема) дисциплины и краткое содержание	Формируемы е компетенции , индикаторы	очная форма			
			Контактная работа обучающихся с преподавателем /из них в форме практической подготовки, часов			Самостоятельная работа, часов
			Лекции	Практические занятия	Лабораторны е работы	
3 семестр						
1	Тема 1. Основные понятия теории сложности	ПК-3 ИД-1, ИД-2	3,0	3,0		3

2	Тема2. Сравнения с одним неизвестным	ПК-5 ИД-1, ИД-2, ИД-3	3,0	3,0		3
3	Тема3. Сравнения второй степени	ПК-3 ИД-1, ИД-2	3,0	3,0		3
4	Тема4. Реализация операции умножения	ПК-5 ИД-1, ИД-2, ИД-3	3,0	3,0		3
5	Тема5. Умножение с помощью быстрого преобразования Фурье	ПК-3 ИД-1, ИД-2 ПК-5 ИД-1, ИД-2, ИД-3	3,0	3,0		3
6	Тема6. Вероятностные алгоритмы проверки чисел на простоту	ПК-3 ИД-1, ИД-2 ПК-5 ИД-1, ИД-2, ИД-3	4,5	4,5		3
7	Тема7. Криптографическая система RSA	ПК-3 ИД-1, ИД-2 ПК-5 ИД-1, ИД-2, ИД-3	4,5	4,5		3
8	Тема8. Дискретное логарифмирование в конечном поле	ПК-3 ИД-1, ИД-2 ПК-5 ИД-1, ИД-2, ИД-3	4,5	4,5		3
	ИТОГО за 1 семестр		27	27		27

6. Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине (модулю)

Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине (модулю) «Технологии обеспечения информационной безопасности» базируется на перечне осваиваемых компетенций с указанием этапов их формирования в процессе освоения дисциплины (модуля). ФОС обеспечивает объективный контроль достижения запланированных результатов обучения. ФОС включает в себя:

- описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;
- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций;
- типовые контрольные задания и иные материалы, необходимые для оценки знаний, умений и уровня овладения формируемыми компетенциями в процессе освоения дисциплины (модуля).

ФОС является приложением к данной программе дисциплины (модуля).

7. Методические указания для обучающихся по освоению дисциплины

Приступая к работе, каждый студент должен принимать во внимание следующие положения.

Дисциплина (модуль) построена по тематическому принципу, каждая тема представляет собой логически заверченный раздел.

Практические занятия проводятся с целью закрепления усвоенной информации,

приобретения навыков ее применения при решении практических задач в соответствующей предметной области.

Самостоятельная работа студентов направлена на самостоятельное изучение дополнительного материала, подготовку к практическим и лабораторным занятиям, а также выполнения всех видов самостоятельной работы.

Для успешного освоения дисциплины, необходимо выполнить все виды самостоятельной работы, используя рекомендуемые источники информации.

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)

8.1.1. Перечень основной литературы:

1. Основы информационной безопасности: учебное пособие для вузов / В. А. Галатенко ; Интернет-университет информационных технологий; Под ред. В. Б. Бетелина .— 4-е изд. — Москва : ИНТУИТ : БИНОМ. Лаб. знаний, 2019. — 205 с.

2. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров ; ПОЛИТЕХ, СПб. политехн. ун-т Петра Великого. — Москва : Юрайт, 2017. — 322 с. : ил., портр. — (Университеты России). — Библиография: с. 319-321. — ISBN 978-5-534-00258-4

8.1.2. Перечень дополнительной литературы:

1. Теоретические основы компьютерной безопасности : учебное пособие для вузов / П. Н. Девянин [и др.] .— Москва : Радио и связь, 2000. — 190 с.

2. Галатенко, В. А. Стандарты информационной безопасности : курс лекций : учеб. пособие / В. А. Галатенко ; под ред. В. Б. Бетелина. — 2- изд. — М. : Интернет- Университет Информационных Технологий, 2006. — 264 с. — (Основы информационных технологий). — Библиогр.: с. 257-263. — ISBN 5-9556-0053-1

8.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине (модулю)

1. Девянин, П. Н. Модели безопасности компьютерных систем : учеб. пособие для студентов вузов / П. Н. Девянин. — М. : Академия, 2005. — 144 с. : ил., табл. — (Высшее профессиональное образование). — Гриф: Доп. УМО. — Библиогр.: с. 139-140. — ISBN 5-7695-2053-1

2. Бабаш, А. В. Информационная безопасность : лабораторный практикум : учебное пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. — 2-е изд., стер. — М. : КноРус, 2013. — 136 с. : ил., портр., табл. — Библиогр. в конце частей. — ISBN 978-5-406-02760-8
//rusmarc

8.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. <http://catalog.ncfu.ru/catalog/ncfu>—Электронный каталог научной библиотеки СКФУ.

2. <http://intuit.ru> — Интуит.

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем

На семинарских и практических занятиях студенты представляют презентации, подготовленные ими в часы самостоятельной работы.

Информационные справочные системы:

Информационно-справочные и информационно-правовые системы, используемые при изучении дисциплины:

1	Информационная справочная система ГАРАНТ.РУ // Режим доступа: http://www.garant.ru/
---	---

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

активные занятия	9-523	Короткофокус.мультимедиа-проектор EpsonEB-536Wi с настен.крепленELPMB45 и наб.каб
	9-429	Монитор ЖК 21,5 DELL черныйDELL E2216H/216H-1941/DELL E2216H21.5 LEDmonitor TN.VGA DP 1920x1080 TiIt Black.3Y
самостоятельная работа	9-410	ПК препод.DeII OptiPiex3040i3-6100 3.7GHz3MDC4(1[4]GB DDR3L1600MHz500GB.GMAHD440 DVD+RW черный с клавиатурой со считывателем смарт-карт телефонно-микрофонной гарнитурой
	9-302	Тонкий клиентDeII Wyse5030для сист.виртуализации рабочих столов на базеVMWareHorizon с аппаратной реализ.протоколаPCoIP с мониторомDELLE2416Hк клавиатурой со считыват. смарт-карт телефонно-микрофонной г

Учебные аудитории для проведения учебных занятий, оснащены оборудованием и техническими средствами обучения. Помещения для самостоятельной работы обучающихся, оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде. Специализированная мебель и технические средства обучения, служащие для представления учебной информации.

Материально-техническая база обеспечивает проведение всех видов дисциплинарной и междисциплинарной подготовки, лабораторной, научно- исследовательской работы обучающихся (переносной ноутбук, переносной проектор, компьютеры с необходимым программным обеспечением и выходом в интернет).

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду образовательной организации.

Особенности освоения дисциплины (модуля) лицами с ограниченными возможностями здоровья

Обучающимся с ограниченными возможностями здоровья предоставляются специальные учебники, учебные пособия и дидактические материалы, специальные технические средства обучения коллективного и индивидуального пользования, услуги ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, а также услуги сурдопереводчиков и тифлосурдопереводчиков.

Освоение дисциплины (модуля) обучающимися с ограниченными возможностями здоровья может быть организовано совместно с другими обучающимися, а также в отдельных группах.

Освоение дисциплины (модуля) обучающимися с ограниченными возможностями здоровья осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья.

В целях доступности получения высшего образования по образовательной программе лицами с ограниченными возможностями здоровья при освоении дисциплины (модуля) обеспечивается:

- 1) для лиц с ограниченными возможностями здоровья по зрению:

- присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе, записывая под диктовку),
 - письменные задания, а также инструкции о порядке их выполнения оформляются увеличенным шрифтом,
 - специальные учебники, учебные пособия и дидактические материалы (имеющие крупный шрифт или аудиофайлы),
 - индивидуальное равномерное освещение не менее 300 люкс,
 - при необходимости студенту для выполнения задания предоставляется увеличивающее устройство;
- 2) для лиц с ограниченными возможностями здоровья по слуху:
- присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе, записывая под диктовку),
 - обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающемуся предоставляется звукоусиливающая аппаратура индивидуального пользования;
 - обеспечивается надлежащими звуковыми средствами воспроизведения информации;
- 3) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата (в том числе с тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):
- письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;
- по желанию студента задания могут выполняться в устной форме.